CHAPTER IX

Digital Dilemma: Difficulties in Detecting Cyber Crime
And Enforcement Of Law

9.0 DIGITAL DILEMMA

9.1 Origin Of The Issues

Two events lead to motivate re-examining the concepts, policies, and practices associated with intellectual property:

1. Advances in technology have produced radical shifts in the ability to reproduce, distribute, control, and publish information. Information in digital form has radically changed the economics and ease of reproduction. Reproduction costs are much lower for both rights holders (content owners) and infringers alike. Digital copies are also perfect replicas, each a seed for further perfect copies. One consequence is an erosion of what were once the natural barriers to infringement, such as the expense of reproduction and the decreasing quality of successive generations of copies in analog media. The average computer owner today can easily do the kind and the extent of copying that would have required a significant investment and perhaps criminal intent only a few years ago.

Computer networks have radically changed the economics of distribution. With transmission speed approaching a billion characters per second, networks enable sending information products world-wide cheaply and almost instantaneously. As a consequence, it is easier and less expensive both for a rights holder to distribute a work and for individuals or pirates to make and distribute unauthorized copies.

The World Wide Web has radically changed the economics of publication, allowing everyone to be a publisher with world wide reach. The astonishing variety of documents, opinion, articles, and works of all sorts on the web demonstrate that millions of people world wide and making use of that capability.

With its commercialization and integration into everyday life, the information infrastructure has run heading into intellectual property law. Today, some actions that can be taken casually by the average citizen—downloading files, forwarding information found on the web—can at times be blatant violations of intellectual property laws; others, such as making copies of information for private use, may
require subtle and difficult interpretation of the law simply to determine their legality. Individuals in their daily lives have the capability and the opportunity to access and copy vast amounts of digital information, yet lack a clear picture of what is acceptable or legal nor is it easy to supply a clear, "bright-line" answer, because (among other things) current intellectual property law is complex.

9.1.1 Why the Issues Are Difficult?

The issue associated with intellectual property (IP) on digital form addressed in this report are difficult for a number of reasons:

- The stakeholders are many and varied. A wide variety of stakeholders present a broad range of legitimate concerns about the impacts of information technology. It is important to understand what these different concerns are and how technology affects these stakeholders. For example, the ability to self-publish on the web may change the interaction between authors and traditional publishers leading to shifts in power.

- Content creators have different agendas, handle IP according to varying strategies, and look for different kinds of return on their investment. Authors have a variety of motivations, different notions of what constitutes a return on their investment, and as a consequence different strategies for handing intellectual property. The traditional model-content produced and sold, either directly or with advertiser support is the most familiar and encourages a view of IP Law as the foundation that provides exclusive rights. But other models include giving intellectual property away in the expectation of obtaining indirect benefit in a positively correlated market (e.g., distributing free web browser software such as Linux and the Apache Web Server), or keeping it private (e.g. establishing trade secrets).

- Fundamental legal concepts can be interpreted differently. For example, significantly different (and emphatic) views exist on whether the nation of "fair use" is to be construed as a defense against a change of infringement or an affirmative right that sanctions copying in specific circumstances'. The difference matters, for both theoretical and pragmatic reasons. If fair use is an affirmative right for instance, than it ought to be acceptable to take positive actions, such as circumventing content protection mechanizing (e.g., decoding an encrypted file), in order to exercise fair use. But taking such positive
actions may well be illegal under the regime of fair use as a defense. The basic point is very controversial, some legal scholars hence labeled as "absurd" the notion that fair use could be an affirmative right.

- Laws and practices vary worldwide, yet networks have global reach. The information infrastructure like the communications networks on which it builds is global, yet there is considerable variation in different countries laws, enforcement policies, and even cultural attitudes toward IP.
- The economics of information products and IP can be subtle. Although content-producing industries account for a sizable and growing portion of the nation's economy and international trade the economic significance of protecting IP is not completely clear. Stronger IP protection could encourage increased levels of creative output resulting in more rapid progress and additional information products.
- But protecting IP also entails costs, including costs for directly related activities such as enforcement, and other less obvious costs. The net economic effects of changes in protection levels are difficult to assess.

9.2 Public Access: Copying and Access

In the digital world, even the most routine access to information invariably involves making a copy; computer programs are run by copying them from disk to memory for example can act that some courts have rules to be "copying" for the purposes of copyright law, and web pages are viewed by copying them from a remote computer to the local machine. But the exclusive right to copy is the first and perhaps most basic right of a copyright holder. How can the conflict be resolved between the desire to provide access to works and the desire to control copying, if, for digital information, access is copying?

This dilemma affects authors and publishers who wish to distribute digital works and need a way to accomplish this, so that the work can be accepted, yet still be protected against unauthorized reproduction. The problem affects policy makers, because the traditional first-sale rule of copyright, an important element of public policy, is undermined by information in digital form. That rule works in the world of physical artifacts because they are not easily reproduced by individuals and are not

---

digital works. Consumers are affected as well, because access is accomplished by copying and in the digital world copyrights' traditional control of copying would mean, control of access as well.

9.3 Mechnisms for Protecting Intellectual Property
9.3.1 Technical Protection Tools

Technical protection tools include a wide variety of software and hardware-based mechanisms that limit access to or use of information. Although these technologies are not widely used for IP protection in 1999; a few tools have been deployed to protect IP in certain niches With some success, for example the digital water making of images, and selected use of exemption, especially in the entertainment industry. Software-based tools have the advantage of ease of distribution, installation, and use. They also have a major drawback because the protected content must eventually be displayed to the user (or somehow "consumed") for its value to be realized. If content is delivered to an ordinary PC, the information displayed can today be captured and copied by any one with sufficient technical knowledge.

A higher level of protection for valuable content in the face of determined adversaries requires special-purpose hardware. This is (impart) the inspiration behind some "information appliances" (e.g. portable players for digital music, portable electronic books) and behind so-called "trusted systems", a combination of software and special hardware. Information appliances are beginning to have an impact in the market and may provide an effective delivery vehicle because they are not general purpose (i.e. programmable) computers, from which displayed content can be captured fairly easily. The trusted system approach, to the extent that it relies on special-purpose hardware incorporated into ordinary PCs, faces the problem of convincing the many users of existing PCs to set aside their investment in existing hardware and buy new devices that will in some ways, be less capable.

The experimental circumvention of technologies asked to protect intellectual property is a common practice in the cryptology and security R & D community, one that enables the development of more efficient and effective protection technologies. This useful practice is threatened by recent developments, notably the digital Millennium Copyright Act (DMCA), which makes circumvention illegal except under certain conditions. The overall approach favoured by the cryptology and security

---

2 Supra 1 - P. 6 - 7
community is to make circumvention legal, while making certain exploitations of successful circumventions illegal (including of course, theft of I.P.). Some members of the committee believe that a number of specific changes are needed to the DMCA.

9.3.2 2. Business Models

Intellectual property protection is often viewed in terms of just law and technology. The law indicates what may be done legally, while technology provides some degree of on-the-spot enforcement. But law and technology are not the only tools available. A third, powerful factor in the mix is the business model. By selecting an appropriate business model, a rights holder can at times, significantly influence the pressure, for and degree of illegal commercial copying and unauthorized reproduction by individuals.

Business models that can contribute to the protection of IP include traditional sells models (low-priced mass-market distribution with convenient purchasing, where the low price and ease of purchase make it more attractive to buy than to copy) and advertiser-supported models (selling readers attention to keep the product price low), as well as the more radical step of giving away IP and selling a complementary product or service (e.g., open source software given away, with consulting and maintenance as the service). Because digital content is difficult to protect; it can be very profitable to find a business model that does not rely primarily on technical protection, or even that exploits tendencies to share and redistribute content.

Digital technology enables the creation of new kinds of information products and services, which raises a multiple of legal issues. Digital repositories pose difficult questions about authorship, ownership and the boundaries among protected works. Additional issues, arise concerning the meaning of digital publication and the distinctions between fair use and private use.

9.4 The Emergence of the Digital Dilemma

The widespread use of computer networks and the global reach of the World Wide Web have added substantially to the information sector’s production of an astonishing abundance of information in digital form, as well as offering unprecedented ease of access to it. The good news is the enrichment that this explosive growth in information brings to society as a whole. The bad news is the

---

3 Supra 1 – P 12-15
4 Supra 1 – P 18
digital information and the web to copy, distribute and use information illegally. The web is an information resource of extraordinary size and depth, yet it is also an information reproduction and dissemination facility of great reach and capability, it is at once one of the World’s largest libraries and surely the World’s largest copying machine. The traditional tool for dealing with use and misuse of information is intellectual property law, the constellation of statutes and case law that govern copyrights, patents, and trade secrets. Part of the case for granting rights in intellectual property (IP) is the belief that protecting IP promotes the development of new products and sciences, and that erosion of these rights could threaten the economic performance of the information sector and curtail the major benefit it has brought.

9.5 AN ENDURING BALANCE UPSET?

The task of intellectual property protection has always been difficult, attempting as it does to achieve a finely tuned balance providing authors and publishers enough control over their work that they are motivated to create and dissemination, while seeking to limit that control so that society as a whole benefits from access to the work. The challenge was elegantly stated some 200 years ago in a legal case in Great Britain:

"We must take care to guard against two extremely equally prejudicial; the one, that men of ability who have employed their time for the service of the community, may not be deprived of their just merits, and the reward of their ingenuity and labour; the other, that the world may not be deprived at improvements, nor the progress of the arts be retarded". In more recent times, a U.S. Court reiterated the significance of balancing rights and access:

We must remember that the purpose of the copyright law is to create the most efficient and productive balance between protection (incentive) and dissemination of information, to promote learning’s, culture and development.

Three recent technological trends are key to the possible upset of the delicate balance of interests in intellectual property – viz., digital information, networks, and the web. A second factor challenging the balance arises from the transformation of the digital information infrastructure into a routine part of everyday life. In the United States, computers and the web have become common-place in work settings and are fast becoming a routine presence in householders; what was once the province of corporations and research laboratories has become a broadly available capability. One

\[5\] Lord Mansfield in Sayree v. Moore, 1785, cited in Kaplan (1967), P.17
\[6\] Supra 1 – P. 23
important consequence is that ordinary citizens are now faced with questions involving the subtleties of intellectual property law, questions they are ill-prepared to answer.

A second consequence of the emergence of the information infrastructure into everyday life is that individuals find themselves capable of reproducing vast amounts of information in private, using commonplace, privately owned equipment. A single individual can now do in private what once would have required substantial commercial equipment and perhaps criminal intent. One important consequence is that copyright law is becoming more concerned with regulating private behavior of individuals. Traditionally, copyright has concerned public actions with public consequences, such as public performance, public display, and dissemination of copies (an inherently public act), and has focused on actions of organizations or individuals (like pirates) whose actions have large-scale public consequences. But with computer and communication equipment becoming common place in the home, the potential impact of the private behavior of individuals has grown, and so correspondingly has interest in regulating the behaviour.

This represents an important consequence of information technology’s emergence into everyday life and presents another social and policy challenge in managing the IP balance.

9.6 Intellectual Property Law is complex:

Complying with IP law presents difficulties in part because of its complexity. Intellectual Property Law is a compendium of general principles (e.g., the exclusive right to reproduction), subtle distinctions (e.g. “idea” versus “expression”) and numerous special case exceptions (e.g. the right to play background music, royalty free, at agricultural fairs). Copyright is complex partly because it deals with intangible rights in intangible subject matters partly because it regulates the activities of a wide variety of industries, and partly because it reflects the results of hard-fought negotiations and industry-specific compromises. Much of the complexity of this law is pertinent only to the specific industry-to-industry dealings is addresses and is irrelevant to the general public. When corporations and lawyers were the ones routinely grappling with copyright laws, the complexity was a burden handled by a relatively specialized audience with appropriate skills and training. Now that the
issues have emerged into the mainstream of daily life, the same complexities are being faced by the people unprepared for them.

Music offers are illustration of the complexity of copyright laws that consumers routinely encounter. Here, for example, is information posted by the Recording Industry Association of America (RIAA) in an attempt to let people know what they can and cannot do. Even the RIAA admits the complexity.

First, for your personal use, you can make analog copies of music. For instance, you can make analog cassette tape recordings of music from another analog cassette, or form a CD, or from the radio or basically from any source. Essentially, all copying onto analog media is generally allowed.

Second, again for your personal use, you can make some digital copies of music, depending on the type of digital recorder used. For example, digitally copying music is generally allowed with minidisk recordings, DAT recorders, digital cassette tape recordings, and some (but not all) compact disk-recordings (or CDR recorders). As a general rule for CD-Rs, if the CR-R recorder is a stand-alone machine designed to copy primarily audio, rather than data or video, then the copying is allowed. If the CR-R recorder is a computer component, or a computer peripheral device designed to be a multipurpose recorder (in other words, if it will record data and video, as well as audio, then copying is not allowed. The commonsense view of intellectual property often conflicts with what the law actually says, leaving even those who wish to act appropriately at a loss to know what to do; the concept of fair use is central to the situations that a thoughtful consumer routinely encounters, what about installing software on two computers, or copying a CD? How does the consumer begin to answer the question of the “nature” of the copyrighted works, or evaluate the impact on the market? If the consumer would have objectively decided that buying a second copy of a CD for the car was not worth the cost, does it follow that making a personal copy is permissible because it would have to market impact? .................. This consumer, having heard of “fair use”, attempts to understand it in the ordinary way (i.e, by dissecting the meaning of the individual terms in the phrase, apparently unaware that the phrase is simply a name for a more complex concept), a common behaviour for people faced with unfamiliar concepts. The response also demonstrates the frustration in the ordinary consumer’s view of the distinction that can arise between law and perceived fairness. The consumer’s attitude here may not be
admissible, but it is not unused and will continue to be a problem as long as the subtleties of intellectual property law intrude on everyday life and as long as those subtleties require difficult judgements.

These problems are not easily remedied in part because of the pace and continuity of technological change.

The Digital Dilemma recognizes the differences in the analog and digital worlds. Specifically, the increased possibility of access to digital works from many points as opposed to access only where the physical copy is located. In the digital world, distance from the copy becomes irrelevant. When a user downloads a digital work and prints or makes disc copies, each of these copies is a perfect copy. While accessibility can be increased because of the availability of digital formats, it also makes private copying of these works easier and more difficult to detect. This is a significant problem for the copyright holder.

Users of copyrighted works become part of the social and cultural record of a civilization, public access is especially important to librarians. The licensing of digital resources as opposed to purchase of the work threatens public access, a core value of librarians and perhaps a core value of the public at large. Not only is public access threatened but also public libraries themselves may be at risk. Information needs to be communicated and shared to be valuable. Certainly, copyright holders deserve fair compensation for their works, but licensing may or may not be fair. In this digitally advanced world we witness the holders of copyright facing tremendous problem and piracy is on the rise.

"Globally, the recoding industry has experienced significant revenue decline and piracy growth within the last five years. In some countries like the United States, piracy is comprised mainly of the digital sharing of the digital recorded music files as MP3s. In other countries recorded music piracy is dominated by the physical production and sale of CD-Rs by organized crime networks. While there have been a number of legislative and law-enforcement changes made in many countries across the globe, these defensive efforts have at best served to show piracy’s growth. The next step for the recoding industry is to develop a recorded digital music strategy for each country in an effort to restore revenue growth and reduce piracy by offering consumers a compelling digital music value proposition.

---

7 Supra 1 - P. 45-48
Robert Hollyman, focuses on the growth problem of digital copying via the Internet. The challenges is, in addition to private enforcement actions. We definitely needed at least two, three times the effort. We have now, for starters’, Holleyman said, if that does not happen, he believes, legitimate business will not survival on the Internet”\textsuperscript{10}.

If copyright is not adequately protected by law and technology, producers won’t be able to sell and distribute the movies, music, and other entertainment.

“Due to numerous advantages of low cost computing, the Internet, and advances in the wireless telecommunication significant challenges face society.

Law enforcement successfully can investigate digital crimes through expanded data analysis, better coordination, specialized training, and dedicated resources. Not only new technologies emerge, but new and altered forms of digital crimes will as well.

In-spite of international law enforcement efforts to cooperate through sharing information, recognizing laws and expanding extradition agreements, digital crime in the future promises to outpace those efforts. One may confidently assert that the future will see a substantial increase in the number of potential targets and potential perpetrators of digital crime \textsuperscript{11}. Another problem in the digital world is the publication of porn in Internet and spread of known child sexual abuse images on-line. Right of privacy is another problem.

On 12-06-2009, “...........Microsoft announced, we are donating photo DNA technology to National Center for Missing and Exploited Children (NCMEC) to help disrupt the spread of known child sexual abuse images on-line. Photo DNA is a technology created by Microsoft Research which helps calculate the distinct characteristics of a digital image in order to match it to another photo of that same image. The license allows NCMEC to make use of the technology and it also allows also allows NCMEC to sub-license, the technology to electronic service providers(ESPs). Preventive measures in India has not been so effective as because the I T Law is virtually silent on it.

Microsoft commends the efforts of law enforcement around the world in the distribution of child sexual abuse images on-line and recognize that the problem is too vast and growing to address talon. It is hope that photo DNA will compliment

\textsuperscript{10} Robert Holleyman, National Journal: Digital Dilemma, August 5, 2005: \url{www.news_story.php3.html}

\textsuperscript{11} P.N. Grabsky & Russel G.Smith: crime in the Digital Age :Published by :Transaction Publishers, Rutgers University, New Brunswick, 1988 : \url{www.int_comp.org}
images. At this time, Microsoft licensing the photo DNA technology to NCMEC to sub-license to ESPs. That said, in the future, we intend to explore the possibility of making this type of technology available to law enforcement”

9.7 Protecting Digital Intellectual Property: Means and measurements

Recent years have seen the exploration of many technical mechanisms intended to protect intellectual property (IP) in digital form, along with attempts to develop commercial products and services based on those mechanisms.

9.7.1 TECHNICAL PROTECTION

The evaluation of technology is challenging the status quo of IP management in many ways. The technical protection services (TPSs) that may be able to assist in controlling, the distribution of digital intellectual property on the Internet.

A number of general points are important to keep in mind about TPSs.

- Technology provides means, not ends; it can assist in enforcing IP policy, but it cannot provide answers to social legal and economic questions about the ownership of and rights over works, nor can it make up for incompletely or badly answered questions:

- No TPS can protect perfectly. Technology changes rapidly, making previously secure systems progressively less secure. Social environments also changes with the defeat of security systems attracting more (or less) interest in the population. Just as in physical security systems, there are inherent trade-offs between the engineering design and implementation quality of a system on the one hand and the cost of building and deploying it on the other. The best that can be hoped for is steady improvement in TPS quality and affordability and keeping a step ahead of those bent on defeating the systems.

- While technical protection for intellectual property is often, construed as protecting the rights of rights holding to collect revenue, this view point is too narrow. Technical protection offering additional important services, including verifying the authenticity of information (i.e., indicating whether it comes from the source claimed and whether it has been altered -- either inadvertently

---

12 Microsoft Donates Photo DNA to NCMEC, January 2, 2010. Posted by Xaviermorgan in Forensic, Law Enforcement- Exploited Children and a comment:http://www.matthewjettfall.com
obvious reasons; publishers are well need authenticity controls to protect their brand quality.

- As with any security system the quality and cost of a TPS should be tailored to the values of and risks to the resources it helps protection
- As with any security system the quality and cost of a TPS should be tailored to the values of and risks to the resources it helps protect: The newest movie release requires different protection than a professor’s class-notes.
- Again, as with any security system, there are different degrees of protection. Some TPSs are designed to keep honest people honest once provide only a modest level of enforcement more ambitious uses seek to provide robust security against professional pirates.
- As with any software, TPSs are subject to design and implementation errors that need to be uncovered by careful research and investigation. Professional cryptologists and digital security experts look for flaws in existing services in order to define better products.
- TPSs almost invariably cause some inconvenience to their users. Part of the ongoing design effort is to eliminate such inconvenience or at least to reduce it to tolerable levels.
- The amount of inconvenience caused by a TPS has been correlated historically with its degree or protection. As a result, in the commercial context, overly stringent protection is as bad as inadequate protection: In either extreme – no protection or complete protection (i.e., making content inaccessible) – revenues are zero. Revenues client with movement away from the extremes the difficult empirical task is finding the right balance.
- Protecting technologies that are useful with special-purpose devices (i.e., cable – television set up boxes or portable digital music players) are quite different from those intended for use in general purpose computers. For method – attached general – purpose computers, software alone cannot achieve the level of technical protection attainable with special purpose hardware. The special purpose devices for protection are:
  1. ENCRYPTION; An underpinning Technology for Technical protection service components. Cryptography is a crucial enabling technology for IP management. The goal of encryption is to scramble objects so that
they are not understanding or usable until they are unscrambled. The technical terms for scrambling and unscrambling are "encrypting and "decrypting". Encryption facilitates IP management by protecting content against disclosure or modification and while it is stored. If content is encrypted effectively, copying the files is nearly useless because there is no access to the content without the decryption key. Software available of the shelf provides encryption that is for all practical purposes unbreakable, although much of the encrypting software in use today is somewhat less robust. Many commercial IP management strategies plan a control role for what is called "symmetrical-key encryption, so called because the same key is used both to encrypt and decrypt the content. Each object (e., movie, song, text, graphic, software application) is encrypted by the distributor with a key unique to that object; the encrypted object can then be distributed, perhaps widely (e.g. placed on a web site). The object key is given only to appropriate recipients (e.g. paying customers), typically via a different, more secure route perhaps one that relies on special hardware.

9.7.2 ACCESS CONTROL IN BOUNDED COMMUNITIES

Perhaps the most fundamental form of technology for the protection of intellectual property is controlling access to information (i.e., determining whether the requester is permitted to access the information). A basic form of such control has been a part of the world of operating systems was first implemented, offering limited but useful security. In its simplest form, an access control system keeps track of the identity of each member of the identities of the data objects, and the privileges (reading altering, executing, and so on) that each user has for each object. The system consults this information whenever it receives a service request and either grants or denies the request depending on what the privilege indicates.

Existing access control, however, offers only a part of what is needed for dealing with collections of intellectual property. Such systems have typically been used to central access to information for only relatively short periods such as a few simple access criteria (e.g.,
read, alter, execute) and for objects whose owners are themselves users and who often close at hand whenever a problem or question arises.

In contrast access control systems for intellectual property must deal with time periods as long as a century or more and must handle the sometimes complex conditions of access and use. A sizable collection—as indeed a digital library will be—also needs capabilities for dealing with hundreds or thousand of documents and large communities of users.

9.8 ENFORCEMENT OF ACCESS AND USE CONTROL IN OPEN COMMUNICATIONS

Access control systems of the sort outlined above can be effective where the central issue is specifying and enforcing access to information, as is typically true in bounded communities represented by, for example a single corporation or a college campus. In such communities much greater emphasis is placed on questions of original access to information than on questions of what is done with the information once it is in the hands of the user. The user is presumed to be motivated (e.g., by social pressure, or community sanctions) to obey the rules of use specified by the rights management information.

A larger problem arises when information is made accessible to an unbounded community as it is routinely on the web. The user cannot in general be presumed to obey rules of use (e.g., copyright restrictions on reproduction); therefore, technical mechanisms capable of enforcing such rules are likely to be needed.

A variety of approaches has been explored. The simpler measures include techniques for posting documents that are easily captured when using existing browsers. One way to do this uses Java routines display content rather than the standard HTML display. This gives a degree of control over content use because the display can be done without making available the standard operating system copy and paste or printing options.

There are also number of increasingly complex techniques for controlling content use that are motivated by the observation made earlier, that digital IP liberates content from medium—the information is no longer attached to anything physical.

Encryption is a fundamental was in this task. At a minimum, encryption requires that the consumer get a decryption key, without which a copy of the
encrypted content is useless. But a digital song, for example, and you get both an encrypted file and a password for decrypting and playing the song.

But this approach secures only the original access to the content and its transit to the consumer. Two additional problems immediately become apparent. First, the concept is still not “attached” to anything physical, so the consumer who wished to do so could pass along (or sell) to others content and the decryption key. Second the consumer could use the key to decrypt the content, save the decrypted version in a file, and pass that file along to others.

On approach to maintaining on site decryption for peripheral devices is illustrated of the Digital Transmission, content protection (DTCP) standard, an evolving standard developed through a collaboration of Hitachi, Intel, Matsushita, Sony, and Toshiba.

9.9 COPY DETECTION IN OPEN COMMUNITIES : MARKING AND MONITORING

When a valuable digital object is not encrypted and is outside the sphere of control of its rights holders, the only technical means of hindering misuse is to change it in ways that discourage wrongdoing or facilitate detection. One technique calls for releasing only versions of insufficient quality for the suspected misuses.

Another technique embeds in the digital document information about ownership, allowed uses, and so on one of the simplest and most straight forward ways to do this is by labeling the document in a standard way (so the label can be found) and in a standard vocabulary (so the terms of use may be widely understood). In its simplest format, a digital label could take the form of a logo, trades mark, or warning label (e.g. May be reproduced for noncommercial purpose only”). Labels are intended to be immediately visible and are a low-tech solution in that they are generally easily removed or changed, offering no enforcements of usage terms.

A second category of label attached to some digital documents is a time stamp used to establish that a work had certain properties at a particular point in time.
Digital time stamping is a technique that affixes an authoritative crypto
graphically strong time stamp to digital content; the label can be used to demonstrate
what the state of the content was at given time\textsuperscript{13}.

"The novel business models and new technologies to protect
intellectual property, as well as education in copyright law are all likely to be more
effective mechanisms than major legislative changes for protecting electronic
information at this time, says a new report from a committed of the National Research
Council of the National Academics. These methods should be used to complement
existing copyright laws that protect owners and distributors of digital information
while maximizing access and use by the public. Digital Intellectual Property is
fundamental to the growth of electronic, and the way it is handled has broad
implications. The question of how to control distribution and use of digital
information is much more than a legal issue alone. Law, business, and technology and
Internet, hence approaching the problem from a single view-point will be inadequate.
Abroad framework is needed to address all aspects of the public and private interest
and to ensure the future vitality of the Internet economy\textsuperscript{14}.

Concluding Comments:

The wide spread use of computer and information and communication technologies, and
global reach of the World Wide Web(WWW) have added substantially to the information
sections, production of an astonishing abundance of information in digital form as well as
offering unprecedented case of access to it. The cyber criminals who take advantage of the
properties of digital information and the web to copy, distribute and use information illegally.

The task of intellectual property protection has always been difficult. Attempt has to be
made to achieve a finely tuned balance providing authors and publishers enough control over
their work that they are motivated to create and dissemination, while seeking to limit that
control, so that society as a whole benefits from access to the work. The policy makers and
stakeholders will have to ensure that the important public purposes embodied in copyright law
continue to fulfilled in the digital context.

\textsuperscript{13} Supra 1 – P. 152-156, 158-161 & 164-165
\textsuperscript{14} NEWS National Research Council: Committee on Intellectual Property Rights and the Emerging Information Infrastructure,